REMARKS

Upon entry of this amendment, Claims 1-42 will be pending in this application. In view of the foregoing amendments and the following remarks, applicant respectfully requests consideration of the new Claims.

Tomlinson et al, (6,532,542) as discussed previously are concerned with the storage and retrieval of data at a central site. In addition to previous arguments these arguments concerning Tomlinson are presented. As per claim 1: Tomlinson is utilizing personal authentication data transmitted to the server to perform work at the server.

As per Claim 2: The comments that the teaching of Tomlinson at Col. 7 lines 5 through 10 are applicable here is not based on foundation because, Tomlinson specifically references the fact that "the smart card could utilize public-key cryptographic techniques" (PKI), whereas, the current invention specifically excludes PKI. The current invention has no need for a central service although, one embodiment utilizes the key generated by the invention to interact securely with the central server.

As per claim 3: At col. 9, line 54, Tomlinson mentions biometric data as an aside to the authentication procedure but the biometric data is not

used by the invention. Many hundred inventions will make use of biometric data but they will not be similar. Tomlinson is specifically concerned with accessing data encrypted on a central server and they are agnostic as to the methodology used for local authentication of the user.

As per claim 7: The examiner has misread Tomlinson at col. 10, lines 1-3 in that the password of the user is transmitted to the central server where it is utilized, whereas in the current invention, the password is used locally and is not transmitted to the server. At col. 10, lines 43-45, Tomlinson does not teach "providing an encrypted data file to the remote computer". At col. 11, lines 2-25, Tomlinson uses the password in the encrypt/decrypt process, but the teaching would not aid in specifying the current invention. While it may be a subtle difference, it is a large difference. Tomlinson is using the password in conjunction with the server to store encrypted user data. The current invention, uses the password in conjunction with a personal storage device to first authenticate the user and secondly to form a unique key.

As per Claim 8: What Tomlinson teaches at col. 7, lines 2-10 is that a smart card vendor might use PKI on the smart card to store data. This teaching is of no value in the current invention, because the interest of the current invention is to teach how to use data to authenticate the user and not to transmit or store data. Tomlinson does teach that a file is

encrypted and stored on the smart card. Tomlinson states "to allow storage of core data items on a smart card" (col. 7, line 5).

As per claim 9: Refer to reference in remarks about claim 3 above.

As per claim 10: As per remarks in claim 3 above, Tomlinson does not teach that the biometric data is a part of the encrypted data file.

As per claim 11: It is not at all clear from Tomlinson at col. 10, lines 30-42, that there is any use made of biometric data in this invention. The examiner appears to be taking a lot of latitude in inferring information that is not contained in Tomlinson.

As per claim 12: Tomlinson does not say that biometric data is in included in any data file!

As per claim 13: Again, Tomlinson does not teach that any biometric data is a part of the encrypted data file. Tomlinson does not teach that there are authenticated user keys. Tomlinson teaches that the keys are authenticated by means of a MAC which is a relatively common manner to authenticate the keys.

As per claims 14 and 15: See claim remarks above for biometric discussion. Col. 12, lines 2-59 refer to the authentication of the application programs. Specifically, they rely upon the "Microsoft

Authenticode calls (line 50) that uses PKI methodology (line 49) and is not considered in the current invention. This section does not deal with the integrity of the encrypted data file!

As per claim 16: Again, the examiner has misread both Tomlinson and the current invention.

As per claim 17: All of these remarks have been discussed above.

As per claim 18: See remarks claim 12 above.

As per claim 19: See remarks claim 3 above.

As per claim 20: See remarks claim 3 above.

As per claim 21: See remarks claim 14 above.

As per claim 22: See remarks claim 3 above.

As per claim 23: At Col 11, lines 7-12, Tomlinson does not discuss "the server configured to receive data encrypted using the authenticated key". Tomlinson teaches of the data that is being encrypted and stored.

As per claim 24: See remarks claim 3 and 8 above.

As per claim 25, 29, 30,33, 36: See remarks claim 12 above.

As per claim 26: See remarks claim 12 above.

As per claim 27, 28: Tomlinson at col. 5, lines 24-28 simply enumerates a number of input devices. It is not clear that the scanner mentioned is even for finger prints because in the manner it is listed it is presumed to be a data entry scanner. At col. 11, lines 7-26, Tomlinson refers to smart cards but the use is not for storing encrypted data files. At col. 10, Tomlinson does make teach of the use of the password based encryption scheme, but this use is more closely aligned to the common practice of password hashing found in most computer operating systems. The current invention uses a completely different methodology for a completely different purpose. The reference to col. 10, lines 15-25 is not apparent to the reader in the context of the current invention and we reject the statement "Tomlinson discuss a biometric reader for generating biometric data of the user (col. 7, lines 6-10)".

As per claim 31, 34, 38: The corresponding item authentication key is simply the hash of the item key and is not in any way associated with the current invention. Tomlinson specifically does not include biometrics in his keys and he makes vague reference to the possibility of using biometrics, leaving the door open for someone to invent the methodology, which is what the current invention does in part: "However, different authentication providers might require different types of responses (such as physical insertion of a hardware token or biometric authentication

procedures)". Again, it is critical to understand that in col. 12, lines 2-59, Tomlinson is discussing the methodology to insure that the application programs are not compromised. This section has nothing to do with encrypting or decrypting data files or storing of data.

As per claim 33, 35, 36,37, 38: Tomlinson does not say that the encrypted data file includes biometric identifying data.

As per claim 40: Refer to claim 8.

As per claim 41: There is some overlap here with Tomlinson, but, the methodology is not similar. It is not clear that you could deduce the current invention from the teaching of Tomlinson.

We can find no similar references in Tomlinson as referred to in the exam: "a decrypt engine in the remote computer for using a password (col 10, lines 1-6)", "provided by the user to decrypt in the remote computer and encrypted data file (col 10, lines 12-15)", "provided by the user into the encryption key of the user (col 10, lines 15-25)". All of these references refer to the procedure for getting the user credentials to the server for server use, not on the local use as claimed by the

examiner. What Tomlinson teaches at col. 7, lines 2-10 is that a smart card vendor might use PKI on the smart card to store data. This teaching is of no value in the current invention, because the interest of the current invention is to teach how to use data to authenticate the user and not to transmit or store data. Tomlinson does teach that a file is encrypted and stored on the smart card. Tomlinson states "to allow storage of core data items on a smart card" (col. 7, lines 2-10).

At col. 9, line 54, Tomlinson mentions biometric data in as an aside to the authentication procedure but the biometric data is not used by the invention. Many hundred inventions will make use of biometric data but they will not be similar. Tomlinson is specifically concerned with accessing data encrypted on a central server and they are agnostic as to the methodology used for local authentication of the user. Their invention begins after local authentication. At col. 9, lines 47-48, "items in protected storage may require user interaction", whereas, in the current invention, user interaction is mandatory in all cases because it is local and not central.

At col. 11, lines 2-25, Tomlinson uses the password in the encrypt/decrypt process, but the teaching would not aid in specifying the current invention. While it may be a subtle difference, it is a large difference. Tomlinson is using the password in conjunction with the

server to store encrypted user data. The current invention, uses the password in conjunction with a personal storage device to first authenticate the user and secondly to form a unique key.

The examiner has misread Tomlinson at col. 10, lines 1-3 in that the password of the user is transmitted to the central server where it is utilized, whereas in the current invention, the password is used locally and is not transmitted to the server. At col. 10, lines 43-45, Tomlinson does not teach "providing an encrypted data file to the remote computer".

Conclusion

In specifying the invention, the Applicant has reviewed the prior art of Thomlinson (6,532,542), Mashayekhi (5,818,936), Ote (6,023,506), and others. None of these would preclude the current invention from being allowed.

The Applicant respectfully request a Notice of Allowability. If the Examiner has questions regarding the case, the Examiner is invited to contact Applicant's undersigned representative at the number given below.

Dated: June 2, 2005 By: _____

5

Lynn D. SPraggs, Ph.D.
Ultra Information Systems Inc.
2179 11th Ave.
Vernon, BC Canada V1T 8V7
Tel: (250) 542-0112
Fax: (250) 549-3751
e-mail: lspraggs@uisamerica.com